UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,218	11/26/2001	Pasi Into Loukas		8034

7590 09/19/2005

Pasi Loukas
Kemintie 969
Rovaniemi, 96700
FINLAND

EXAMINER	
CHEN, SHIN HON	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/993,218	LOUKAS, PASI INTO	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 28-46 are examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

   a) The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 28-46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claims 29-46 recite the limitation "a said identification" in terms used throughout the claims. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

   A person shall be entitled to a patent unless –

   (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 28-34, 36-38, and 44 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Hypponen et al. U.S. Pub. No. 20030191957 (hereinafter Hypponen).

7. As per claim 28, Hypponen discloses a network based web content identification and control system especially for wide area networks, like the Internet, comprising: client computer(s), which are any computers in the network (Hypponen: [0006]-[0010]); examiner host computer(s), which are any computers in the network chosen for that purpose, and which each examine web content remotely by processing tiny sized delivered identifications of said web content locally (Hypponen: [0006]-[0010]; [0032]); wherein identification(s) of file(s) or other web content is delivered from a client computer to an anti-virus host computer (Hypponen: [0006]-[0010]; [0035]); wherein identification(s) of web content is delivered to an examiner host computer either before, during, or after a client computer receives said web content from the network (Hypponen: [0006]-[0010]); wherein said anti-virus host computer compares each of said delivered identification(s) to stored identifications of files or other web content, and on the basis of the results of said comparison either: (a) it is performed safety measures, (b) and/or, said client computer and/or the user of said client computer is informed about the results of said comparison, (c) or, no specific actions are performed (Hypponen: [0006]-[0010] and [0035] and [0038]: intercept the data and identify if the data is of a type capable of containing a virus); wherein said web content comprises files, web pages, e-mail messages, e-mail message attachments or any data which a client computer can acquire from the network (Hypponen: [0032]).

8. As per claim 29, Hypponen discloses a network based anti-virus system according to claim 28, Hypponen further discloses the system comprising: wherein a said stored identification either: (a) belongs to a specific file or other web content, (b) does not belong to any specific

file or other web content, but is rather an identification filter, (c) or, partly belongs to a specific file or other web content, and partly is a identification filter (Hypponen: [0035]).

9. As per claim 30, Hypponen discloses a network based anti-virus system according to claim 28. Hypponen further discloses the system comprising: wherein said delivered identification comes from said client computer, from the respective source host computer of the web content, or partly from said client computer and partly from the respective source host computer of the web content (Hypponen: [0006]-[0010]; [0035]: intercept the data and check).

10. As per claim 31, Hypponen as modified discloses a network based anti-virus system according to claim 28. Hypponen further discloses the system comprising: wherein a said delivered identification consists of file identification information and/or, data identification information (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein a said stored identification consists of file identification information and/or, data identification information (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said file identification information comprises one or more of the following properties of the file or other web content to which said file identification belongs: (a) source URL-address or other type of address, (b) source computer URL-address or other type of address, (c) name, (d) type, (e) content type, (f) size, (g) creation date, (h) version number, (i) publisher, (j) authentication certificate, (k) or, other properties (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said data identification information of the file or other web content to which said

data identification belongs, comprises: (a) a check-sum or any identification value based upon the data of said file or other web content. (b) and / or, data sample picked according to a certain pattern, algorithm or other rule from said file or other web content, (c) or, all data of said file or other web content (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said file identification information and said data identification information is delivered to said anti-virus host computer either: (a) solely from said client computer, (b) solely from the respective source host computer(s) of said file(s) or other web content which file identification information anal data identification information it is question of, (c) or, partly from said client computer and partly from said respective source host computer(s) (Hypponen: [0006]-[0010]).

11. As per claim 32, Hypponen discloses a system according to claim 31. Hypponen further discloses the system comprising: wherein said safety or preventive measures are performed when a said delivered identification matches or resembles in certain extent any of said stored identification (Hypponen: [0006]-[0010]; [0035]-[0038]).

12. As per claim 33, Hypponen discloses a system according to claim 32. Hypponen further discloses wherein said stored identification belong to known virus infected web content (Hypponen: [0035]).

13. As per claim 34, Hypponen discloses a system according to claim 33. Hypponen further discloses the system comprising: wherein said safety measures including one or more of the

following: (a) preventing the download of the examined web content to the client computer, (b) performing a virus scan on the examined web content in the client computer or in the examiner host computer, (c) destroying the examined web content (Hypponen: [0035]-[0038]).

14. As per claim 36, Hypponen discloses a system according to claim 33. Hypponen further discloses the system comprising: intermediate computer(s), which are any computers in the network capable to intercept data which client computers receiver from the network (Hypponen: [0035]); wherein said delivered identification(s) is delivered to the examiner host computer by a said intermediate computer (Hypponen: [0035]-[0038]).

15. As per claim 37, Hypponen discloses a system according to claim 36. Hypponen further discloses the system comprising: wherein said safety measures include one or more of the following: (a) the intermediate computer preventing the download of the examined web content to the client computer, (b) the intermediate computer performing a virus scan on the examined web content, (c) the intermediate computer destroying the examined web content (Hypponen: [0035]-[0038]).

16. As per claim 38, Hypponen discloses a system according to claim 36. Hypponen further discloses the system comprising: wherein said intermediate computer is (a) a server of the local area network, (b) a server of the internet service provider, (c) or a network node computer (Hypponen: [0013]).

17. As per claim 44, Hypponen discloses a system according to claim 28. Hypponen further discloses wherein said client computers are host computers into which data is uploaded (Hypponen: [0031]).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 35 and 39-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen in view of Bates et al. U.S. Pat. No. 6721721 (hereinafter Bates).

20. As per claim 35, Hypponen discloses a system of claim 34. Hypponen does not explicitly disclose the system comprising: wherein the examiner host computer calculates an estimate for the security threat level of the examined web content and informs it to the client computer or the user of the client computer. However, Bates discloses determine trustworthiness of a file (Bates: column 10 lines 9-39). It would have been obvious to one having ordinary skill in the art to allow the examiner host computer to determine whether a file poses threat or not before being transmitting the file to the client. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates within the system of Hypponen because it allows files to be analyzed prior to being forwarded to client.

21. As per claim 39, Hypponen discloses a network based anti-virus system according to claim 32. Hypponen discloses the system comprising: wherein said stored identifications of files are stored identifications of known non-wanted/unacceptable files; wherein said stored identifications of other web content are stored identifications of other known non-wanted / unacceptable web content (Hypponen: [0035]: file type). In addition, Bates more explicitly discloses a anti-virus database used to store virus status information including the types of file, name of the file, checksum, timestamp, etc. so that an URL can be checked prior to deliver the content to client device (Bates: column 13 lines 24-42). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include more information to detect potential virus infected file that are not complicated including the name and types of virus files because types of file and names of the file are simple criteria to detect potential virus infected files. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates within the system of Hypponen because it improves the efficiency and resources of central anti-virus server to detect malicious files.

22. As per claim 40, Hypponen as modified discloses a system according to claim 39. Hypponen as modified further discloses wherein said preventive measures include preventing the download of the examined web content to the client computer, and/or destroying the examined web content (Hypponen: [0035]-[0038]).

23. As per claim 41, Hypponen as modified discloses a system according to claim 39. Hypponen as modified further discloses the system comprising: intermediate computer(s) , which are any computers in the network capable to intercept data which client computers receive from the network (Hypponen: [0035]); wherein said delivered identification(s) is delivered to the examiner host computer by a said intermediate computer (Hypponen: [0035]-[0038]).

24. As per claim 42, Hypponen as modified discloses a system according to claim 41. Hypponen as modified further discloses the system comprising: wherein said preventive measures include the intermediate computer preventing the download of the examined web content to the client computer, and/or the intermediate computer destroying the examined web content (Hypponen: [0035]-[0038]).

25. As per claim 43, Hypponen as modified discloses a system according to claim 41. Hypponen as modified further discloses wherein a said intermediate computer is: (a) a server of the local area network, (b) a server of the internet service provider, (c) or, a network node computer (Hypponen: [0013]).

26. Claims 45 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen in view of Bates and further in view of Bates et al. U.S. Pat. No. 6785732 (hereinafter Bates2).

27. As per claim 45, Hypponen discloses a network based download information system especially for wide area network, like the Internet, comprising: a client computer (Hypponen: [0031]); a host computer keeps database of the identifications of the files and / or other web content which the client computers or the users of client computers have downloaded from the network, each said identification being stored in said database in connection of the respective downloading of said file or other web content to which said identification belongs (Hypponen: [0035]); wherein said anti-virus host computer retains information about one or more of the following: (a) old and / or newly detected virus infections, (b) old and / or newly detected security threats, (c) old and / or newly determined security risk ratings, (d) personal download statistics, for the files and / or other web content which a client computer or the user of said client computer has earlier downloaded from the network (Hypponen: [0035]); wherein said anti-virus host computer informs / alerts the respective client computer and / or the user of said respective client computer, when said anti-virus host computer retained information on the part of any of (a) through (c) changes in certain way (Hypponen: [0038]). In addition, Bates also discloses above limitations (Bates: column 12 lines 24-42). Hypponen as modified does not explicitly disclose said client computer and / or the user of said client computer being optionally able to access said anti-virus host computer retained information; wherein if said anti-virus host computer announces said anti-virus host computer retained information on the part of any of (a) through (c) to have changed alarming enough for certain files(s) or other web content, then the respective client computer optionally: (a) destroys said file(s) or other web content from said client computer, (b) and / or, performs a virus scan in said client computer, the software for said virus scan optionally provided by said anti-virus

host computer. However, Bates2 discloses the server may download virus checker to client and the client may perform the security measures and database is provided to store information about newly found virus including file location, names, etc. (Bates2: column 2 lines 34-56). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to notify the client so that the client can check/scan the file for virus upon notification by the server because the virus checker can be centralized or decentralized. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates2 within the combination of Hypponen-Bates because it reduces the burden of the server to check files of all clients.

28. As per claim 46, Hypponen as modified discloses a system according to claim 45. Hypponen as modified further discloses wherein the client computer destroys the host computer appointed harmful web content and/or performs a virus scan (Bates2: column 2 lines 34-56).

Response to Arguments

29. Applicant's arguments filed on 7/3/05 have been fully considered but they are not persuasive.

Regarding to applicant's argument, applicant argues that the reference does not have collection of identification information. However, the term identification information can be defined as file type, file name, file extension, etc. Therefore, applicant's argument is respectfully traversed because the claim language does not allow one of ordinary skill in the art to differentiate the term "identification information" and the terms used in prior art.

Furthermore, applicant has argued that the prior art of record does not produce the novelty achieved by present invention. However, applicant has argued many aspects of the invention that is not specifically claimed in the claim language. Therefore, applicant is advised to incorporate certain limitations into the claims.

Conclusion

30. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100